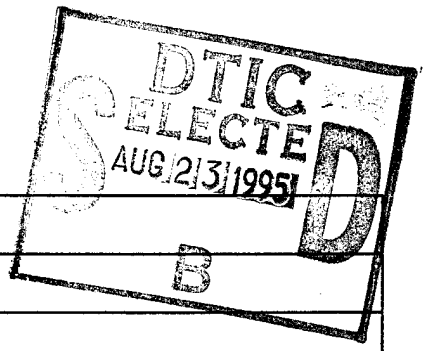
UNCLASS

Security Classification This Page



REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED	
2. Security Classification Authority:	
3. Declassification/Downgrading Schedule:	
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.	
5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT	
6. Office Symbol: C	7. Address: NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207
8. Title (Include Security Classification): A Combatant Commander's Organizational View of Information Warfare/Command and Control Warfare (U)	
9. Personal Authors: Joanne Sexton, CDR USN	
10.Type of Report: FINAL	11. Date of Report: 16 MAY 1995
12.Page Count: 27	
13.Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.	
14. Ten key words that relate to your paper: Information Warfare (IW), C2W, national information policy, USACOM, JC2WC, NIWA, FIWC, AFIWC, LIWA	

15.Abstract: Information warfare (IW) and Command and Control Warfare (C2W) are widely recognized as describing how the U.S. will fight its future wars. Of the two, IW remains undefined; whereas, C2W is finely detailed in joint publications. Despite the inadequate IW definition, the combatant commanders have crated an IW/C2W Cell built around the five elements of C2W (OPSEC, Deception, PSYOP, EW, and Destruction). From this stepping stone, the combatant commanders will evolve into a more comprehensive strategy to incorporate IW. An essential step to this evolution is the need for the combatant commander to fully understand the ramifications of 7 key issues/questions: 1) Why the U.S. must have a national information policy; 2) What organization should take the lead if the continental U.S. suffers a devastating IW attack; 3) What is the peacetime role of IW; 4) Who should take the military IW lead; 5) Who should have the responsibility to prevent redundant IW programs; 6) What should the national security guidance be on black programs; and 7) How should C2-protect programs be improved. When solved, the seven issues will dictate what future organization and role the military will have in IW. The key for the combatant commander is to comprehend the seven issues and seek to shape their solution.

16.Distribution / Availability of Abstract:	Unclassified X	Same As Rpt	DTIC Users
18.Abstract Security Classification: UNCLASSIFIED			
19.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT			
20.Telephone: 841-6457		21.Office Symbol: C	

Security Classification of This Page Unclassified

NAVAL WAR COLLEGE
Newport, R.I.

A COMBATANT COMMANDER'S ORGANIZATIONAL VIEW OF INFORMATION WARFARE AND COMMAND AND CONTROL WARFARE

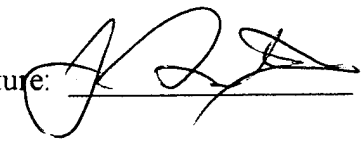
by

Joanne Sexton

CDR USN

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: 

16 June 1995

Paper directed by Captain D. Watson
Chairman, Joint Military Operations Department

_____ _____
Faculty Advisor Date
(Full name of Faculty Advisor & Academic Title)

19950822 098

Abstract of
A COMBATANT COMMANDER'S ORGANIZATIONAL VIEW
OF INFORMATION WARFARE/COMMAND AND CONTROL WARFARE

Information warfare and Command and Control Warfare (C2W) are widely recognized as describing how the United States will fight its future wars. Of the two, information warfare remains undefined; whereas, C2W is finely detailed and fully defined in joint publications. Despite the inadequate information warfare definition, the combatant commanders have created an Information Warfare/C2W organizational cell built around the five elements of C2W (OPSEC, Deception, PSYOP, EW, and Destruction). From this stepping stone, the combatant commanders will evolve into a more comprehensive strategy to incorporate information warfare. An essential step to this evolution is the need for the combatant commander to fully understand the ramifications of the following Information Warfare/C2W issues and questions: 1) Why the United States must have a national information policy; 2) What organization should take the lead if the continental United States suffers a devastating, widespread information warfare attack; 3) What is the role of information warfare during peacetime; 4) Who should take the military information warfare lead; 5) Who should have the responsibility to prevent redundant information warfare programs; 6) What should the national security guidance be on black programs; and, 7) How should C2-protect programs be improved. When solved, these seven issues will dictate what future organization and role the military will have in information warfare. The key for the combatant commander is to comprehend these seven issues and seek to shape their solution.

Codes
A-1

PREFACE

I am headed to an information warfare job in Washington, D.C. My purpose in writing this paper was motivated by pure self-interest. In order to be effective at my next job, I needed to understand why information warfare is currently undefined; Why did the military create Command and Control Warfare (C2W) as a new warfare area; Who are the players in the information warfare game and how do they interface with each other; How are the commander in chiefs (CINC) organized to incorporate Information Warfare/C2W into a CINC level warfighting strategy; Who do the CINCs turn to for help; and, Why are each of the military services creating its own information warfare center? This paper attempts to answer these questions. In addition, seven key issues from the CINC's perspective are identified that will shape the future military use of information warfare.

This paper is written from the CINCs perspective. Due to page limits, I choose to focus on a single CINC to portray the current CINC Information Warfare/C2W organization. Commander in Chief, U.S. Atlantic Command (USACOM) was picked as the sample CINC organization, because the Joint Staff identified USACOM as one of the CINCs that had gotten the furthest in defining its Information Warfare/C2W organization.

For current and future readers, it must be recognized that this paper is written in a time when no formal joint doctrine exists that tells a CINC how to organize to succeed in its Information Warfare/C2W mission. A CINC's current, best guidance, which cannot be quoted or formally referenced because it has not been accepted for final publication, is a second draft of Joint Publication 3-13, "Joint Doctrine for Command and Control Warfare (C2W) Operations" of 1 September 1994 with a Joint Publication preliminary coordination

third draft of the same publication expected to be distributed for initial review in May 1995.

As a further note to the reader, the use of the term "combatant commander" throughout this paper refers to the commander in chiefs of each of the nine Unified CINCs. This particular usage of the term combatant commander directly corresponds to the Doctrine for Joint Operations (Joint Pub 3-0) of 9 September 1993 which defines the term combatant commander as referring to the commander in chief of both geographical and functionally organized combatant commands.

Finally, I would like to thank Col J.R. Gray of the Joint Command and Control Warfare Center (JC2WC), Lt Col Paul Gregory of U.S. Atlantic Command (USACOM), and Lt Col Steven Spano of the Joint Staff (J-6) for their assistance in helping me understand the very complex subject of information warfare and how the military is integrating its use into a workable military strategy and organizational framework.

Introduction

As of the Persian Gulf War, information warfare and Command and Control Warfare (C2W) are widely recognized as describing how the United States will fight its future wars. Of the two, information warfare remains undefined; whereas, C2W is finely detailed and fully defined in joint publications. The Chairman of the Joint Chiefs of Staff (CJCS) Memorandum of Policy 30 defines C2W as:

> "[t]he integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW) and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade or destroy adversary C2 capabilities, while protecting friendly C2 capabilities against such actions. Command and Control Warfare applies across the operational continuum and all levels of conflict[1]."

As this definition points out, C2W has both an offensive (counter-C2) and defensive (C2-protect) aspect.

From the military viewpoint, "C2W is the military strategy that implements [i]nformation [w]arfare on the battlefield...[2]" and is considered as offering "the commander the potential to deliver a KNOCKOUT PUNCH before the outbreak of traditional hostilities[3]."

The reason why definitions are so important is because an organization needs understanding before it can effectively organize to take advantage of a new capability. In the case of Information Warfare/C2W, the military does not have a solid understanding of what information warfare is; yet, the military found it had to create an organizational structure in order to take advantage of the capabilities of this new warfighting area as soon as possible. Just how one combatant commander--Commander in Chief (CINC), U.S. Atlantic Command (USACOM)-- organized to implement Information Warfare/C2W is the focus of this paper.

In addition, seven Information Warfare/C2W issues, from the combatant commander's perspective, are identified. When solved, these seven issues will dictate what future organization and role the military will have in information warfare. The key for the combatant commander is to comprehend these seven issues and seek to shape their solution.

But first, let's understand why a definition of information warfare has proved so elusive.

Why Information Warfare is so Hard to Define

The United States military and national policy makers have struggled to precisely define information warfare. Four reasons exist to explain this difficulty--1) information warfare applies to more than the battlefield, i.e., the military alone cannot define information warfare; 2) an extensive number of federal agencies and Department of Defense elements play a role in information warfare, i.e., the definition of information warfare must be reached by consensus; 3) the United States is still being transformed by the information revolution; and, 4) the definition of information warfare requires a reassessment of the balance of power between the rights of private citizens and the power given to the government to protect them.

Information warfare is not limited to just the battlefield, but includes projecting and protecting United States national strength in information technology at home and abroad. What happens if the United States is attacked by an adversary using a software penetration mechanism like a Virus, Worm, Trojan horse, or Trap door--a form of information warfare. Whether widely recognized or not, the United States is extremely vulnerable to these types of software attacks--a vulnerability that is only increased with greater United States global connectivity, growing interconnectivity between United States civilian and military computer

networks and telecommunication systems, and heavier reliance on information and its assured flow to run our military, economy, society, and political infrastructures.

Let's consider the consequences if the following systems were targeted in the United States for disablement: financial markets, nuclear power plants, telephone systems, electronic power distribution systems, traffic lights, or air traffic control and airline reservations systems. Who would be in charge of cleaning up the mess and be responsible for restoring order? If the software attack were a computer crime, the first to be called would probably be the Federal Bureau of Investigation (FBI) and Secret Service, with expected oversight from the Justice Department and Commerce Department[4]. If the attack were conducted over INTERNET, the Computer Emergency Response Team at Carnegie Mellon University would swing into action[5]. If the attack were initiated by an international terrorist group, foreign government, or international criminal organization, the Central Intelligence Agency would play a role given its charter to assess foreign intentions and capabilities to conduct information warfare against the United States[6].

Should the United States military be involved? And, if so, should all the military services play a role or just some? The Office of the Assistant Secretary of Defense for C^3I (ASD-C^3I) has the job of establishing the policy of how the military services will react in these situations, as well as, determining what role the military services will play in information warfare as a whole. It has already been determined that if military networks are attacked or used to launch a software attack, then the expertise of the Defense Information Systems Agency (DISA) and the National Security Agency (NSA)--specifically the Automated

Systems Security Incident Support Team, as well as, the joint DISA-NSA Center for Information Systems Security[7] --would be called upon.

Given the different possible scenarios and number of players potentially involved, information warfare requires wide interagency coordination. This need for interagency interdependency to manage and implement information warfare helps explain why a definition of information warfare has been so difficult to achieve.

A further reason for the non-definition is, the United States is in the process of transformation[8]. As a nation, we are still trying to grasp the impact the information revolution is having on our society, economy, and political systems. Within this context, it is challenging to understand what information warfare can do for the United States and what can happen to us if information warfare were applied against our nation.

The biggest reason, however, why information warfare remains undefined is because of the balance of power issue. What is at stake is determining a fine line between citizen privacy and the amount of government power needed to ensure national and economic security. Paradoxically, information warfare puts the United States at risk; however, to protect itself, the United States may need to lessen its protection of its private citizen's personal security. A case in point is the Clipper chip. The government and law enforcement officials believe they need the Clipper chip to fight computer crime and ward off computer espionage. These officials view Clipper --"...which is supposed to offer phone privacy to consumers while providing police access--as a good way to give the public powerful encryption while still preserving law enforcement's ability to conduct electronic

surveillance[9]." Personal privacy advocates contend that Clipper makes it too easy for the government to snoop.

A comprehensive definition of information warfare will require the United States to debate just what our nation stands for. The United States government and military were established to protect the rights of citizens--imagine trying to get a bill passed in Congress that attempts to lessen what American's have come to understand as our "tradition" of personal privacy.

Given the firm definition of C2W and the understandable still evolving definition of information warfare, let's now take a look at how one combatant commander choose to configure its Information Warfare/C2W organization.

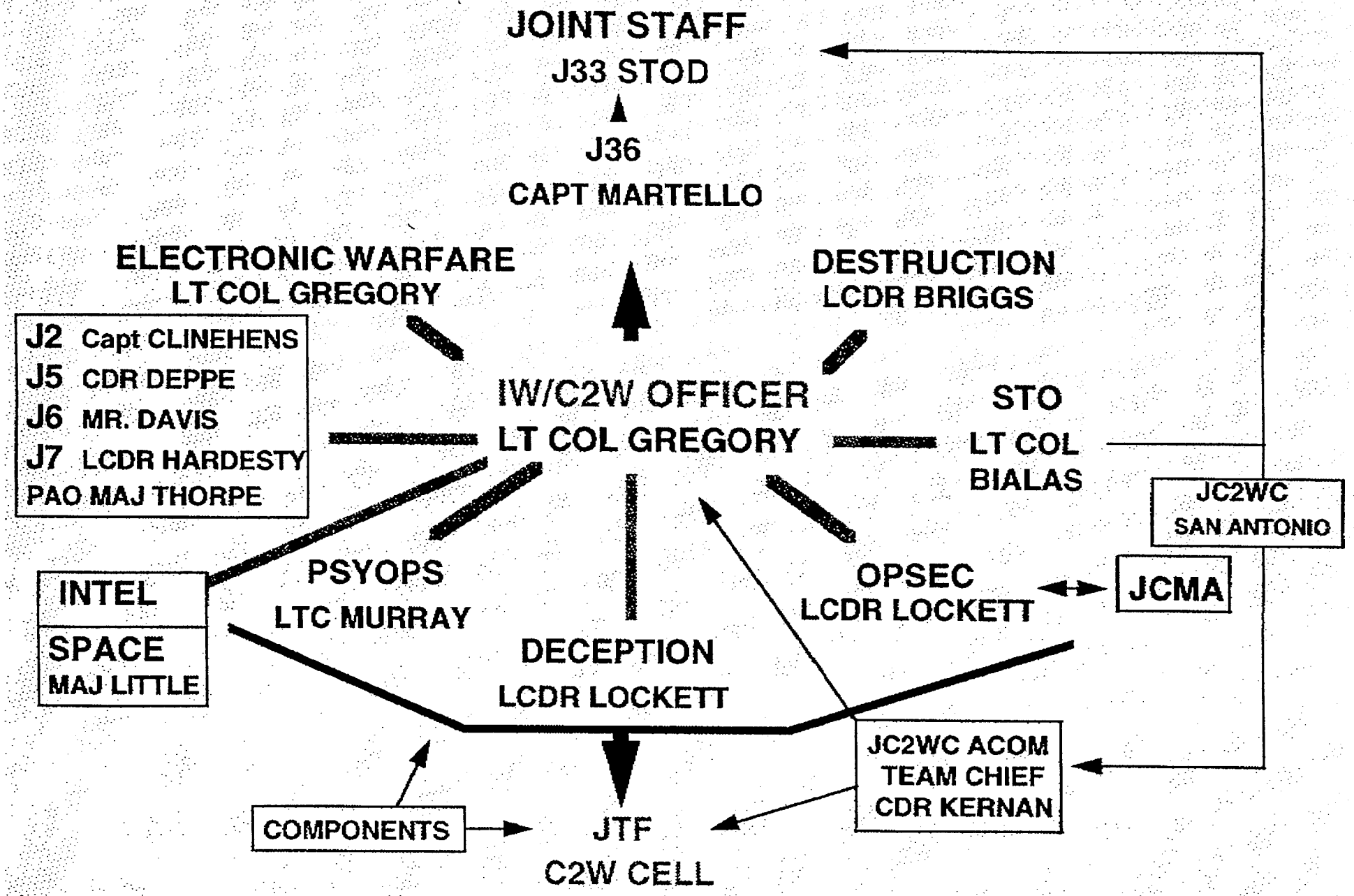
How is USACOM Organized for Information Warfare/C2W

USACOM created a single staff component, the Information Warfare/C2W cell, to ensure Information Warfare/C2W operations are fully integrated into joint operational planning and extensively coordinated among the many elements of the joint headquarters and component service staffs. Figure 1[10] depicts the USACOM Information Warfare/C2W cell structure. Each of the elements in the figure are described below. The description starts with the center of the figure and moves clockwise around the diagram.[11]

LT COL Gregory is the USACOM's Information Warfare/C2W Officer. An Electronic Warfare F-4G Wild Weasel operator/pilot by trade, LT COL Gregory views his role as a Information Warfare/C2W facilitator in service to Joint Task Force (JTF) staffs, the USACOM staff as a whole, and the USACOM service components. It is LT COL Gregory's

FIGURE 1

USACOM IW/C2W CELL ARCHITECTURE



specific responsibility to ensure Information Warfare/C2W is well planned, coordinated, and jointly integrated at the operational level.[12]

LT COL Gregory directly interfaces with both J-3 Operations Directorate and J-6 Command, Control, Communications and Computer Systems Directorate of the Joint Staff. J-3 and J-6 have a shared responsibility to support on-going Information Warfare/C2W policy efforts, to build the Information Warfare/C2W doctrine, and to formulate the future Joint Staff Information Warfare/C2W strategy[13]. Other J-codes help (J-2, J-5, J-7, and J-8), but the main Information Warfare/C2W focus is centered within J-3 and J-6.

Certainly, either J-3 or J-6 would prefer the lead in developing this new warfare area. Both have a sizable stake in Information Warfare/C2W policy development and implementation. Politically, it has proven too difficult to consider the joining of these two codes or giving the lead to one code only. Making a decision in this regard would tip the military's hand as to who should have the military information warfare lead--the operators (J-3) or the "Information Warriors"[14] (J-6). It is, however, not too far fetched to consider a future Joint Staff that has a whole different set of J-codes in order to meet the new responsibilities of this warfare area. Currently, the Joint Staff must be classified as in the learning stage of how best to organize to implement Information Warfare/C2W.

LT COL Gregory organized the USACOM Information Warfare/C2W cell around the five pillars of C2W (EW, Destruction, OPSEC, Deception, and PSYOPS). An O-5/O-4 warfare specialist is assigned to each of these positions; and, as a whole, the staff fully represents the joint nature of CINC operations.[15]

In addition to the five pillars, LT COL Bialas is the Special Technical Operations (STO) Officer. STO is the white world liaison that interfaces with the highly classified black programs associated with information warfare. In addition to the jobs already described, LT COL Gregory has found a need to establish an Intel/Space focal point, a position that will be filled in September 1995; and, is working on identifying a position and candidate for a computer/communications expert (J6 background).[16]

The Joint Command and Control Warfare Center (JC2WC), located in San Antonio, Texas, plays a critical C2W support role to the CINCs. Although the USACOM Information Warfare/C2W Cell is quite capable, LT COL Gregory would like to add manpower and expertise to his staff. In times of crisis, the JC2WC provides an already established means to do this. The JC2WC provides augmentation to the CINC staff and JTF. During the Haiti Operation (Uphold Democracy), JC2WC sent seven personnel plus computer equipment to augment the USACOM Information Warfare/C2W Cell. JC2WC also helped round out the Haiti Operation JTF C2W staff with needed expertise and experience. This ready support is available by calling a single point of contact that has been established for each Unified CINC. In the case of USACOM, LT COL Gregory contacts CDR Kernan for any needed JC2WC support.[17] Appendix A provides a detailed description of the JC2WC mission.

The Joint Communications Security (COMSEC) Monitoring Activity (JCMA), an element of NSA, can be tasked by LT COL Gregory to provide COMSEC monitoring and analysis support during exercises and actual operations. The purpose of COMSEC monitoring is to identify exploitable vulnerabilities and to recommend countermeasures and

corrective action. JCMA offers the combatant commander a way to reduce risk and provide a level of C2 protection.[18]

The USACOM Information Warfare/C2W Cell provides the JTF what assistance is needed, as well as, technical advice. Planning is done by the JTF, e.g. the 82nd Corp did the bulk of the planning for Operation Haiti. If the JTF has an C2W issue it cannot handle, then it gets the Information Warfare/C2W Cell involved. If LT COL Gregory's staff cannot resolve the issue, then the Joint Staff is called. Although USACOM can directly interface with other agencies for information warfare support, LT COL Gregory has found using the Joint Staff to interface with the Washington agencies (DISA, NSA, etc.) beneficial in terms of ease and quickness of support provided.[19]

Service components provide the assets used to conduct C2W. LT COL Gregory acts as a facilitator to source--find the right service to provide--the required assets during crises and regular exercises. The actual tasking of resources is done at the service level, because the components are more aware of available deployment levels of any given unit.[20]

The Information Warfare/C2W Cell has defined interfaces with J-2, J-5, J-6, J-7, and the Public Affairs Officer. The J-2 interface is to ensure timely collection, processing, tailoring, and dissemination of intelligence to C2W elements. For certain C2W operations, intelligence evaluation of C2W program effectiveness must also be arranged. J-5 coordination ensures C2W is developed into long range plans. The J-6 interface provides needed communications and computer support, as well as, planning for C2-protection measures. The current need echoed by anyone within Information Warfare/C2W is the continuing need to educate the force on the importance of expanding the military's C2-protect capability. J-7

plays a major role in this regard along with integrating C2W into joint exercises. Finally, the Public Affairs Officer must have a working knowledge of C2W operations in order to deconflict public affairs programs with on going C2W operations.[21]

With this brief overview of how USACOM is organized to complete its Information Warfare/C2W mission, let's now examine why each of the services have created a service specific information warfare center.

Why Service Information Warfare Centers Exist

CJCS Memorandum of Policy 30 directed Chiefs of the Services and CINC, U.S. Special Operations Command (USCINCSOC) to "designate a staff component to act as a single working-level point of contact for C2W..."[22] In response to CJCS Memorandum of Policy 30, each of the services have either created or are in the process of establishing information warfare centers. In general, these centers are to develop service specific Information Warfare/C2W doctrine, as well as, build and maintain service Information Warfare/C2W capabilities that combatant commanders can task as required. A brief description of each of the services' information warfare centers is provided in Appendix B for future reference.

It would be easy to look at the establishment of each of the service information warfare centers and label them redundant. With the way the current Department of Defense system is set up, each of the service information warfare centers are required. Only the services can buy things and develop new technologies. Only the services develop doctrine for its forces. Only the services create the forces and the capabilities that the combatant commanders tap to meet joint operational mission needs. Until the Department of Defense

system changes, each of the services must have its own information warfare center to ensure its forces can provide the combatant commander the Information Warfare/C2W support they need. An effective approach, is the Air Force's early initiative to have Navy and Army personnel assigned to JC2WC. This influence, may well serve as a model to the Navy and the Army. The more joint these centers become the more likely is it that the services can create greater interoperability between service systems and prevent redundant capabilities from being created.

The military has achieved a workable, initial Information Warfare/C2W organization despite an inadequate definition of information warfare. By no means, is the current organization the most effective possible nor the ultimate organization. We can expect the organization to continue to evolve as the military and the nation further grapples with the question what is information warfare and what is its impact on the military and the nation as a whole. One thing for sure, the military's development of C2W cannot be considered anything less than masterful. By concentrating on the definition of C2W, as opposed to the much larger and nebulous definition of information warfare, the military has built an organization around known, well-understood capabilities. This C2W organization is now being used as a stepping stone to understand and incorporate the larger construct of information warfare.

Through the step-wise approach, the combatant commanders have made headway in understanding information warfare. The next step is tied to comprehending the seven issues. Let's take a look at what they are.

Information Warfare/C2W Issues

The number one issue, from the perspective of the combatant commander, is the United States lacks a national information policy. Surprisingly, the lack of a national policy is understandable. It is tied to the balance of power issue already addressed. Until the United States is ready to reassess and make a stand for what the nation believes is the right level of privacy rights, the hope for a guiding national information policy will remain unfulfilled.

Associated with this issue is, the United States has specific laws that decree that the United States military will not be involved in law enforcement. If the military is being considered to help combat information warfare waged against the continental United States, then posse commitas will need a thorough review and potentially a new definition of the law may be required.

The other six issues are: 1) What organization should take the lead if the United States is attacked domestically; 2) What is the role of information warfare during peacetime; 3) Who should take the military information warfare lead; 4) Who should have the responsibility to prevent redundant programs; 5) What should the security guidance be on black programs; and, 6) How should C2-protect programs be improved. The crafting of a national information policy would help resolve all but the sixth issue.

1) What organization should take the lead?

As evidenced from the earlier scenario, information warfare is an interagency concern. Of the agencies involved, each has a significant piece of the action, but no organization has overall control. Agencies are self-assigning information warfare missions based on traditional roles and in some cases are growing into new areas of responsibility. The possibility of

mission overlap under this system is enormous. The only thing that is keeping the whole system together is the informal, universal agreement across agency lines to network and educate others to the importance of information warfare. As a nation, it is risky to rely on the networking skills of a few individuals to make information warfare into a national strength. A national information policy would broaden the net and more clearly establish areas of responsibility and chains of command and control.

Designating a single government agency to be in charge of information warfare is imperative if the United States is to effectively respond to a widespread, highly destructive software attack--a recovery that must be quick and ensure minimum impact to the population. Not only must a lead agency be assigned, but supporting organizations must understand how best to coordinate its efforts with other action agencies. A national policy would outline both roles and ensure unity of command and unity of effort throughout the crisis.

Actions required to mop up after a destructive software attack against the United States would be similar to actions taken in response to domestic emergency disasters. Those thinking of how best to respond to a national software attack or are actually tasked to draft a national software attack response plan would do well to study Hurricane Andrew and its aftermath or any recent disaster.

Without a national policy, no software attack clean-up plan will be developed nor practiced. This is of significant concern to the Unified CINCs, especially USACOM; CINC U.S. Pacific Command (USPACCOM); and CINC, U.S. Transportation Command (USTRANSCOM). Each of these CINCs have specific responsibilities assigned to them in support of domestic disaster relief[23]. Although the military does not take a lead role in

emergency response, the military heavily supports all disaster assistance efforts; and, more than likely, would be called upon to aid in a software attack clean-up effort.

2) What is the role of information warfare during peacetime?

CJCS Memorandum of Policy 30 declares that Information Warfare/C2W can be used before the start of hostilities to prevent war[24]. To do that, a national information policy of the United States must establish the desire to pursue offensive Information Warfare/C2W against other nations. Although a number of possibilities exist, the offensive act used may be a software attack against another nation's computer networks, a media barrage to emphasize the United States point of view, or a demonstration against another nation's command and control system. Regardless of method chosen, extensive knowledge of the targeted country's computer networks and telecommunication systems, unbiased cultural understanding of the nation under attack, or a nodal analysis of the country's military command and control network is required. None of these examples may be used without significant manpower, capabilities, and time being expended prior to its actual use.

What individuals or organization will perform this analysis? Consider as well, the need to track who is targeting the United States. The combatant commander of the area under analysis should have a say on how this collection is conducted. At present, lack of a national information policy leaves this issue open to time consuming debate and the mission potentially uncovered.

3) Who should take the military information warfare lead?

The Joint Staff and the CINCs have taken a best shot at determining a reasonable Information Warfare/C2W organization. Critics bemoan the coordinator role of the

Information Warfare/C2W officer on the CINCs staff, because coordinators are felt to lack the authority needed to direct tasking of supporting elements. However, considering the lack of a national policy and confusion over what is information warfare, a coordinator role may prove to be the best way to start.

The coordinator role skirts another problem--who should take the military information warfare lead--Operations (J-3) or C^4I (J-6). There is pro and con to either selection. The best hope is to see a future combination of both codes that takes advantage of the strengths of each perspective. Without this benefit, if the desire is to use information warfare as a tool in the warfighters tool box, then the trigger pullers (J-3) need to be in charge or else the capability may go unused.

4) Who should have the responsibility to prevent redundant programs?

Without a national policy to divide the Information Warfare/C2W into specific functional mission areas, the onus is on the military services to prevent Information Warfare/C2W program redundancies. This is a tall order given the United States current downsizing environment and the recognition that information warfare is one of the few growth areas. Budget lines and assigned mission are at stake. The Department of Defense acquisition system needs overhaul. Until the system can be revamped, the military services have no choice, but to pursue the current course. The Joint Requirements Oversight Council's assessment program, however, may prove to be an important first step towards reform.

5) What should the security guidance be on black programs?

A lack of national policy also hurts the development of required security guidance on Special Technical Operations. ASD is both responsible to craft a Department of Defense wide information warfare policy and determine how much the combatant commanders can be told about black programs[25]. How much combatant commanders know about black program tactics, techniques, and sources will determine the degree to which CINCs can play in the information warfare arena.

6) How should C2-protect programs be improved?

Finally, although not directly related to a lack of a national information policy, C2-protect requires greater attention at the CINC level[26]. As evidenced by the Persian Gulf War, the United States possesses an impressive offensive (counter-C2) arsenal. A possible irony of the same war is the United States may have been so successful attacking Iraq's command and control that we may have missed the point of how vulnerable we really are. The goal of the combatant commander is to not let this war lesson go unlearned, but to make the C2-protection side equally capable as its formidable offense minded cousin.

Conclusion

Many complain that the coordinator role of the combatant commander's Information Warfare/C2W Officer is the wrong way to go. Considering our current imperfect understanding of information warfare, it may be the best choice. But, the clock is ticking. Hopefully, the United States will not have to suffer a software attack akin to the Oklahoma City bombing before crafting its national information policy.

APPENDIX A: JOINT COMMAND AND CONTROL WARFARE CENTER (JC2WC)

The JC2WC is a field agent of the Joint Chiefs of Staff. Functionally, the JC2WC works for the J-3, Operations Directorate, but is also a staff element of J33-STOD. STOD stands for Special Technical Operations Directorate and deals with classified black programs associated with information warfare. In its staff role, the JC2WC provides technical expertise and resolution as required.[27]

The mission of the JC2WC is to provide direct C2W support to unified commands, JTFs, functional and service components, and subordinate combat commanders. Support is also given to the Office of the Secretary of Defense, the Joint Staff, the military services, and other government agencies.[28] The JC2WC is the first organization that the joint CINCs turn to with questions on information warfare and C2W.

The JC2WC grew out of the Joint Electronic Warfare Center (JEWC) that had a long established history of providing electronic warfare support to the nine unified commands. The name change reflects the expanded mission of the JC2WC, as well as, the importance of the new joint C2W warfigher area. "The JC2WC supports the integration of OPSEC, PSYOP, military deception, EW, and destruction throughout the planning and execution phases of operations,"[29] "...in addition to its tradition role in developing hardware and simulations[30]." In accomplishing this role, the JC2WC maintains specialized expertise in C2W system engineering, operational applications, technical analytic support, capabilities, and vulnerabilities[31].

The JC2WC is equally staffed by all four services and includes civil service personnel and representatives from three allied nations[32]. The bulk of the military personnel assigned to the JC2WC are operators--pilots, tank drivers, ship drivers and infantry as well as professional intelligence. This operational bent ensures the JC2WC understands what people in the field need.[33] It also ensures believed and immediately accepted expertise when these same operators augment a theater C2W planning cell or assist a JTF as part of a JC2WC regionally focused C2W team.

In support of the combatant commander, the JC2WC has established a Team Chief (liaison officer) for each of the nine Unified CINCs. The JC2WC Team Chief directs a staff of experts representing each of the five elements of C2W. When the team deploys, the Team Chief directs the efforts of the JC2WC personnel assigned to both the CINC staff and JTF.[34]

The JC2WC deployed team not only provides technical augmentation, but also provides well-established continuity that can be a real plus to a recently created JTF. The JC2WC deployment team provides the following further advantages: knowledge of the CINC's tasking, complete knowledge of the CINC's area of responsibility, a pre-established relationship, Special Technical Operations interface, communications connectivity with JC2WC (real time or near real time connectivity for technical support as required), and computer assets. The JC2WC also deploys at no cost to the CINC[35].

The JC2WC provides further support to CINC C2W needs by its ability to quickly acquire new hardware systems. For example, the JC2WC's System Engineering Directorate was able to develop and field, within 53 days, a secure, pocket size rescue beacon which can receive and transmit Global Positioning System location data. This new development was

generated when it was learned that Iraq could track downed flight crews during the Persian Gulf War. This same directorate keeps an eye on emerging government laboratory and industry technology that may be used to meet operational needs.[36]

APPENDIX B: SERVICE INFORMATION WARFARE CENTERS

Air Force:

The Air Force was the first to build its center. The Air Intelligence Agency (AIA) established the Air Force Information Warfare Center (AFIWC) on 10 September 1993 at Kelly AFB, Texas. "The AFIWC was created through a merger of the Air Force Electronic Warfare Center and the security functions of the Air Force Cryptologic Support Center[37]." The Air Force receives tremendous synergistic effect by having the AFIWC co-located with its intelligence arm and the JC2WC. Of interest, the commander of the AIA also serves as the director of the JC2WC[38].

The AFIWC is a large organization of 900 plus officer, enlisted, and civilian personnel. The AFIWC mission description is as follows:

> "Develops, maintains and deploys Information Warfare/Command and Control Warfare (IW/C2W) capabilities in support of operations, campaign planning, acquisition and testing. Acts as time-sensitive, single focal point for intelligence data and C2W services. Provides technical expertise for computer and communications security. Air Force focal point for Tactical Deception and Operations Security Training[39]."

The AFIWC's is made up of four directorates, the main function of each follows: 1) Operations Support Directorate maintains "...the ability to quickly deploy Information Warfare Support Teams to support combat operations[40]"; 2) C2W Database Directorate "...continually maintains select, critical databases to support combat operations, wargaming, testing and acquisition[41]"; 3) Systems Analysis Directorate "...provides quantitative analysis through modeling and simulation of offensive and defensive C2W and information warfare capabilities[42]"; and, 4) Engineering Analysis Directorate improves "...the effectiveness of

information, sensor and weapon system[s] for C2W by providing technical support for US and allied systems[43]". Under the Engineering Analysis Directorate is the Air Force Computer Emergency Response Team which provides consultation and resolution of computer security problems around the clock. Considering the AFIWC staffing, it should come as no surprise that the JC2WC calls upon the AFIWC to help meet some of the JC2WC's commitments[44]. It is expected that once the other service information warfare centers stand-up and provide unique capabilities that the JC2WC will also call upon them to assist the combatant commanders and national-level authorities.

Navy:

The Navy's approach has been to create two centers--the Fleet Information Warfare Center (FIWC) and the Naval Information Warfare Activity (NIWA), each with its own unique focus. Let's take a look at the mission's of each of these activities.

The FIWC will:

> "[a]ct as the Fleet CINC's principal agent for development of IW/C2W tactics, procedures, and training, under the operational control of Commander in Chief, U.S. Atlantic Fleet (CINCLANTFLT), additional duty to Commander in Chief, U.S. Pacific Fleet (CICNPACFLT), Commander in Chief, U.S. Naval Forces Europe (CINCUSNAVEUR), and Commander, U.S. Naval Forces Central Command (COMUSNAVCENT). Deploy personnel trained in the IW/C2W disciplines of exploit, protect, and attack with appropriate counter-C2/C-2 protect hardware and software systems to support battle group and joint task force operations[45]."

The FIWC will be located in Norfolk, Virginia and its projected establishment date is September 1995. The FIWC will be created "...by merging the present Command and Control Warfare Groups Atlantic/Pacific and the Electronic Warfare Operational Programming Facility[46]." FIWC's focus is on the fleet and support to joint operational commanders. The

FIWC will augment and assist deploying units, the Navy shore establishment, and Marine Units with qualified Information Warfare/C2W personnel. FIWC is chartered to develop integrated tactics, techniques, procedures, and training to fleet and shore units and coordinate these actions with joint centers and other service Information Warfare/C2W centers.[47] The FIWA will also,

> "[w]hen requested by CINCLANTFLT, CINCPACFLT, CINCUSNAVEUR, COMUSNAVCENT, provide qualified, trained, and properly equipped IW/C2W personnel to the Joint Commander's Staff. These personnel should be prepared to assist in the planning and execution of joint IW/C2W[48]."

The NIWA was established on 18 August 1994 from a portion of the Naval Security Group Command and is projected to move to Ft. Meade, Maryland by November 1995[49]. NIWA's mission is to guide the Navy "...in its efforts to understand and implement the tenets of information warfare[50]." Specifically, NIWA is tasked to "[a]ct as CNO's principal technical agent and interface to Service and national level agencies engaged in the pursuit of information warfare technologies[51]." NIWA's role is to both keep abreast of new developments in information warfare and to act as the Navy's technical agent and interface for the development and aquisition of systems and techniques associated with Special Technical Operations[52].

Army:

The Army is in the process of standing up the Land Information Warfare Center (LIWC) at Ft. Belvoir, Virginia. The Army had found that its information warfare activities were scattered throughout the Army. Establishment of the LIWC will help centralize and

focus the various aspects of Army information warfare--intelligence, counter intelligence, and command, control, and communications at one location[53].

Although the Army has been slower than the other services to establish an information warfare center, the Army more than makes up for this apparent slowness by how well the Army has integrated information warfare into its doctrine and ethos of every soldier. FM 102-5 offers visionary doctrine which clearly speaks for the need and advantage of information warfare and virtually every soldier is aware of the importance of the digital battlefield.

NOTES

1. Chairman of the Joint Chiefs of Staff, Command and Control Warfare, Memorandum of Policy No. 30, (Washington: 1993), p. 2.

2. Ibid., p. 3.

3. Ibid., p. 5.

4. Winn Schwartau, Information Warfare: Chaos on the Electronic Superhighway. (New York: Thunder's Mouth Press, 1994), p. 409.

5. Ibid.

6. R. James, Woolsey, U.S. Congress, Senate, Senate Selection Hearings, Federal Document Clearing House Congressional Testimony of January 10,1995.

7. Pat Cooper, "DOD Escalates War Against Computer Hackers," Defense News, 1-7 Aug 1994, p. 9:4.

8. General Gordon R. Sullivan and Colonel James M. Dubik, War in the Information Age (Carlisle Barracks, PA: U.S. Army War College, 1994), pp. 6-7.

9. Vic Sussman, "Policing Cyberspace," U.S. News & World Report, 23 January 1995, p. 58.

10. Facsimile from U.S. Atlantic Command, USACOM IW/C2W Cell Diagram, 5 May 1995.

11. Telephone conversation with Lt Col Paul Gregory, USACOM Information Warfare/C2W Officer, Norfolk, VA, 5 May 1995.

12. Ibid.

13. LT COL Bill Percival and LTC Billy Hogan, "Joint Staff Approach to Information Warfare," Brief, Joint Education Conference, Washington, D.C.: 8-9 February 1995.

14. Martin C. Libicki and James A. Hazlett, "Do We Need An Information Corps?," Joint Force Quarterly, Autumn 1993, p. 92.

15. Telephone conversation Gregory.

16. Ibid.

17. Ibid.

18. Ibid.

19. Ibid.

20. Ibid.

21. Ibid.

22. Memorandum of Policy No. 30, p. 23.

23. Koburn C. Stoll, "Translating Policy into Action, the Federal Military Response to Domestic Disasters," NWC 2237, p. 14.

24. Memorandum of Policy No. 30., p. 5.

25. Telephone conversation with Lt Col Steven Spano, Joint Staff (J-6), Washington, D.C., 4 May 1995.

26. Telepone conversations Spano and Gregory.

27. Telephone conversation with Col J.R. Gray, Deputy Director for Operations East, JC2WC, San Antonio, Texas, 5 May 1995.

28. Facsimile from Joint Command and Control Warfare Center, Joint Staff Fact Sheet, 28 April 1995.

29. Ibid.

30. "JEWC Takes on New Name to Fit Expanded Duties," Aviation Week and Space Technology, 10 October 1994, p. 54.

31. Facsimile from Joint Command and Control Warfare Center.

32. Ibid.

33. "JEWC Takes on New Name to Fit Expanded Duties," p. 54.

34. Telephone conversation with Col Gray.

35. Ibid.

36. "JEWC Takes on New Name to Fit Expanded Duties," p. 54.

37. Craig Johnson, "Information Warfare--Not a Paper War," Journal of Electronic Defense, August 1994, p. 56.

38. "EW Expands into Information Warfare," Aviation Week & Space Technology, 10 October 1994, p. 47.

39. Facsimile from Air Force Information Warfare Center, AFIWC Mission Description, 26 April 1995.

40. Johnson, p. 58.

41. Ibid.

42. Ibid.

43. Ibid.

44. Ibid.

45. U.S. Navy Dept., Implementing Instruction for Information Warfare/Command and Control Warfare (IW/C2W) OPNAVINST 3430.26, (Washington: 1995), pp. 8-9.

46. Ibid., p. 8.

47. Ibid., p. 9.

48. Ibid., p. 10.

49. "Going Beyond Real-Time, The Next Step in Simulation," Aviation Week & Space Technology, 12 September 1994, p. 71.

50. Robert Holzer, "U.S. Navy Begins Information War Effort," Defense News, 29 August-4 Sept 1994, p. 9:4.

51. OPNAVINST 3430.26, p. 10.

52. Ibid., pp. 10-11.

53. "Services Gear Up for Information War," Defense Daily, 8 Sept 1994, p. 184:377.

BIBLIOGRAPHY

Chairman of the Joint Chiefs of Staff. Command and Control Warfare. Memorandum of Policy No. 30. Washington: 1993.

Clapper, LTGen. James R. and Trevino, LTC Eben H., Jr. "Critical Security Dominates Information Warfare Move." SIGNAL, March 1995, pp. 71-72.

Cooper, Pat. "DOD Escalates War Against Computer Hackers." Defense News, 1-7 Aug 1994, p.9:4.

"EW Expands into Information Warfare." Aviation Week & Space Technology, 10 October 1994, p. 47.

Facsimile from Air Force Information Warfare Center, AFIWC Mission Description, 26 April 1995.

Facsimile from Joint Command and Control Warfare Center, Joint Staff Fact Sheet, 28 April 1995.

Facsimile from U.S. Atantic Command, USACOM IW/C2W Cell Diagram, 5 May 1995.

"Going Beyond Real-Time, The Next Step in Simulation." Aviation Week & Space Technology, 12 September 1994, p. 71.

Holzer, Robert. "U.S. Navy Begins Information War Effort." Defense News, 29 August-4 Sept 1994, p. 9:4.

"JEWC Takes on New Name to Fit Expanded Duties." Aviation Week and Space Technology, 10 October 1994, p. 54.

Johnson, Craig. "Information Warfare--Not a Paper War." Journal of Electronic Defense, August 1994, p. 56.

Joint Chiefs of Staff. Doctrine for Joint Operations. Joint Pub 3-0. Washington: 9 September 1993.

Joint Chiefs of Staff. Joint Doctrine for Command and Control Warfare (C2W) Operations. Joint Pub 3-13. Second Draft. Washington: 1 September 1994.

Joint Chiefs of Staff. Joint Doctrine for Command and Control Warfare (C2W) Operations. Joint Pub 3-13. Preliminary Coordination Draft. Washington: May 1995.

Kirin, Stephen J. "FEMA's Role in Hurricane Andrew: A Case Study in Crisis Management." Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1995.

Libicki , Martin C. and Hazlett, James A. "Do We Need An Information Corps?" Joint Force Quarterly, Autumn 1993, p. 92.

Percival, LT COL Bill and Hogan, LTC Billy. "Joint Staff Approach to Information Warfare." Brief. Joint Education Conference, Washington, D.C.: 8-9 February 1995.

Schwartau, Winn. Information Warfare: Chaos on the Electronic Superhighway. New York: Thunder's Mouth Press, 1994.

"Services Gear Up for Information War." Defense Daily, 8 Sept 1994, p. 184:377.

Stoll, Koburn C. "Translating Policy into Action, the Federal Military Response to Domestic Disasters." NWC 2237.

Sullivan, General Gordon R. and Dubik, Colonel James M. War in the Information Age. Carlisle Barracks, PA: U.S. Army War College, 1994.

Sussman, Vic. "Policing Cyberspace " U.S. News & World Report, 23 January 1995, p. 58.

Telephone conversation with Col J.R. Gray, Deputy Director for Operations East, JC2WC, San Antonio, Texas. 5 May 1995.

Telephone conversation with Lt Col Paul Gregory, USACOM Information Warfare/C2W Officer, Norfolk, VA. 5 May 1995.

Telephone conversation with Lt Col Steven Spano, Joint Staff (J-6), Washington, D.C. 4 May 1995.

U.S. Navy Dept. Implementing Instruction for Information Warfare/Command and Control Warfare (IW/C2W). OPNAVINST 3430.26. Washington: 1995.

Woolsey, R. James. U.S. Congress. Senate. Senate Selection Hearings. Federal Document Clearing House Congressional Testimony of January 10,1995.